#14

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No. : 09/429,174 Confirmation No. (None)
Applicants : Jung-Chih Huang, et al.
Filed : October 28, 1999
Title : PRE-BOOT SECURITY CONTROLLER
TC/A.U. : 2134
Examiner : Christopher J. Brown

Docket No. : 2139
Customer No.: 23320

DECLARATION OF BRIAN OH

I, BRIAN OH declare that:

1. I am 38 years old and reside at 273 Saratoga Avenue, Santa Clara, California 95050.

2. In 1987, Chun-Buk National University, in Korea, granted me a Bachelors of Science degree in Electronics Engineering.

3. From January 1987, until December 1992, I was employed by Daewoo Telecom, Ltd. in Seoul, Korea as a Hardware Engineer designing main boards for computers which used Intel x86 microprocessors.

4. From January 1993, until August 1995, I was employed by Daewoo Telecom, Ltd. in Santa Clara, California as a Hardware Engineer designing a sound card and docking system for notebook computers which used Intel x86 microprocessors.

5. From September 1995, until March 1997, I was employed by ACC Micro of Santa Clara, California as a Senior System Engineer debugging chipsets for personal computers and providing customer support, and designing a PCMCIA ATA flash controller.

6. From April 1997, until February 1998, I was employed by Trident Microsystems of Mountain View, California as a Senior Application Engineer in a multimedia marketing group debugging integrated circuits and providing customer support.

7. From March 1998 until the present I have been employed by O_2 Micro, Inc., the assignee of the present patent application, as a Senior Application Engineer designing integrated circuits for a CardBus Controller and for Universal Serial Bus ("USB") products, debugging prototype integrated circuits, and providing customer support.

8. I am a joint inventor with Jung-Chih Huang, Yishao Max Huang, Sterling Du and Aaron Reynoso of the invention disclosed and claimed in the present patent application, and am a co-applicant with them for this patent application.

9. I have reviewed:

a. the Office Action that issued for this patent application on January 14, 2004;

b. the references cited in the January 14, 2004, Office Action; and

c. a response to a prior Office Action for this patent application which was received by the United States Patent and Trademark Office ("USPTO") on October 17, 2003.

10. Based upon my review of the January 14, 2004, Office Action, it appears that there exists a lack of appreciation for the structure and operation of the present invention in comparison with

the references applied in rejecting the patent application's claims.

11. This patent application's invention is:

> an integrated circuit pre-boot security controller that includes a non-volatile password memory for storing at least one user password. A password input circuit, included in the pre-boot security controller, receives a password for comparison with any user passwords recorded in the password memory. If the pre-boot security controller is in a security operating mode, a digital logic circuit, also included in the pre-boot security controller, compares the received password with any user passwords recorded in the password memory. If the password received by the password input circuit matches a user password recorded in the password memory, an output circuit of the pre-boot security controller, that is coupled to the digital logic circuit, transmits an output signal to a power subsystem to enable energizing operation of a digital computer.

12. The January 14, 2004, Office Action rejects pending claims 1-18 based upon combinations of United States Patent no. 5,251,304 entitled "Integrated Circuit Microcontroller With On-Chip Memory and External Bus Interface and Programmable Mechanism for Securing the Contents of On-Chip Memory" which issued on a patent application filed in the names of James M. Sibigtroth, Michael W. Rhoades, George G. Grimmer, Jr. and Susan W. Longwell ("the Sibigtroth, et al. patent") either:

a. with United States Patent no. 4,604,708 entitled "Electronic Security System for Electronically Powered Devices" that issued on August 5, 1986, on a patent application filed by Gainer R. Lewis ("the Lewis patent");

b. with:

i. the Lewis patent; and

ii. United States Patent no. 5,313,639 entitled "Computer With Security Device for Controlling Access Thereto" which issued May 17, 1994, on a patent application filed by George Chao ("the Chao patent"); or

c. with

i. the Lewis patent;

ii. the Chao patent; and

iii. United States Patent no. 5,594,319 entitled "Battery Pack Having Theft Deterrent Circuit" that issued January 14, 1997, on a patent filed by Iilonga P. Thandiwe ("the Thandiwe patent").

13. It is readily apparent, merely from the titles of the Lewis, Chao and Thandiwe patents, that their respective inventions all attempt to provide security for electrically powered devices, i.e. attempt to bar unpermitted use of electrically powered devices.

14. Based upon my analysis of the Lewis, Chao and Thandiwe patents specifically set forth below, it is clear that the inventions respectively disclosed in those patents provide only an illusion of security.

15. Conversely, in comparison with the inventions respectively disclosed in the Lewis, Chao and Thandiwe patents, the invention

disclosed in the present application provides true security for electrically powered devices.

16. For the Lewis patent, if an in-circuit emulator ("ICE"), such as that disclosed in United States Patent No. 5,900,014 entitled "External Means of Overriding and Controlling Cacheability Attribute of Selected CPU Accesses to Monitor Instruction and Data Streams" ("the '014 patent") that issued May 4, 1999, were coupled to the microcomputer 10 disclosed in the Lewis patent, the ICE could be used to read out the "predetermined primary security code stored in PROM 34."[1]

17. For the Chao patent, the casing (1) can be easily removed from the disk drive receiving space (40) and replaced by an identical substitute casing which holds a known password in the replacement casing's ROM unit (32).

18. Also for the Chao patent, the casing (1) may be merely removed, and jumpers substituted for the relay unit (331, 341, 351) thereby entirely eliminating any need for entering a password.

19. For the Thandiwe patent, the secure battery system described in the Thandiwe patent can be avoided merely by connecting to the host device 12 a substitute battery pack (10) having a known password stored in its memory 26.

20. Also for the Thandiwe patent, a battery pack entirely lacking the microcontroller circuit 20 and the logic circuit 28 can

[1] See the '014 patent for a more complete description of how an ICE may be used to acquire data that is being accessed by a microprocessor.

be connected to the host device 12 for energizing its operation without any need for entering a password.

21. For the preceding reasons, clearly the security inventions respectively disclosed in of the Lewis, Chao and Thandiwe patents, individually by themselves, can be easily defeated in the simple ways described above, and therefore provide only an illusion of security.

22. The text of the January 14, 2004, Office Action at the bottom of page 4 expressly combines the Sibigtroth, et al. patent with only the Lewis patent stating:

> Sibitroth (sic) discloses a controller and memory as part of an integrated circuit (Sibitroth [sic] Col 2 lines 19-25). It would be obvious to one skilled in the art to construct the microcomputer of Lewis in the method of Sibitroth because it is more compact.

23. I am unable to find in the January 14, 2004, Office Action any express combination of the Sibigtroth, et al. patent with:

a. the Chao patent; or

b. the Thandiwe patent.

24. The Lewis patent clearly discloses that the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with a predetermined primary security code, i.e. predetermined primary password, stored in PROM 34. (Col. 3, lines 50-53)

25. The Sibigtroth, et al. patent discloses a data processing system 10 that includes an integrated circuit package portion 11

and a peripheral portion 12 having an external peripheral device. (Col. 2, lines 19-22)

26. As described in col. 2 of the Sibigtroth, et al. patent at lines 22-25, the integrated circuit package portion 11 includes:

a. a memory 13;

b. a data processor 14;

c. a decoder 16;

d. an instruction inhibit circuit 18; and

e. a programmable security device 20.

27. Attached hereto as Exhibit A is a copy of FIG. 1 of the Sibigtroth, et al. patent that has been annotated with a dashed line that encloses the integrated circuit package portion 11 of the data processing system 10. (Col. 2, lines 26-49)

28. The Abstract of the Sibigtroth, et al. patent discloses that integrated circuit package portion 11 operates in three different modes:

a. a "secure mode;"

b. a "single chip mode;" and

c. an "expanded mode."

29. When the integrated circuit package portion 11 operates in the "secure mode," the data processor 14 with memory 13 within the single integrated circuit package portion 11:

a. restricts instruction access to memory 13 contained within the integrated circuit package portion 11;

b. while allowing data accesses to:

i. either the internal memory 13; or

ii. to a memory external to the integrated circuit package portion 11. (Abstract)

30. When the integrated circuit package portion 11 operates in the "single chip mode," the data processor 14 accesses both data and instructions strictly from within the integrated circuit package portion 11. (Abstract)

31. When the integrated circuit package portion 11 operates in the "expanded mode," the data processor 14 may access either the internal memory 13 or external memory for both instructions and data. (Abstract)

32. If constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action retains the PROM 34 for storing the predetermined primary security code, i.e. predetermined primary password, then **the predetermined primary password may be easily obtained using an ICE as the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with the predetermined primary security code, i.e. predetermined primary password, stored in PROM 34**. (Col. 3, lines 50-53)

33. Therefore, **constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action does not alter the security provided by the invention disclosed in the Lewis patent if the predetermined primary security code, i.e.**

predetermined primary password, is stored in the PROM 34 external to the Sibigtroth-style microcomputer 10.

34. Furthermore, if constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action retains the PROM 34 for storing the predetermined primary security code, i.e. predetermined primary password, then **it will be no more compact than the disclosure of the Lewis patent**.

35. Consequently, constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action **is more compact and betters the security provided by the Lewis patent only if the predetermined primary security code, i.e. predetermined primary password, were stored in the memory 13 of the integrated circuit package portion 11**.

36. In the secure mode of operation of the Sibigtroth, et al. patent's integrated circuit package portion 11, instruction read cycles performed by the data processor 14 are confined to the data processor (sic)[2] as in the single chip mode, whereas data reads and writes initiated by the data processor 14 can be made either internal or external to the data processor 14 as in the expanded mode of operation. **The secure mode of operation provided by the Sibigtroth, et al. patent is an effective and economical solution**

[2] It appears that this text is incorrect, and should correctly read "confined to the integrated circuit package portion 11."

to isolate instruction information of a data processor while allowing the data processor to read or write non-proprietary data external to the data processor.

* * *

However, regardless of the variety of operations considered permissible within a single chip or expanded mode of operation, the functionality of the secure mode insures that memory 13 may not be read or modified by unauthorized sources external to the single integrated circuit package. (Col. 4 lines 38-60)

37. Referring now to Exhibit A, i.e. FIG. 1 of the Sibigtroth, et al. patent, it is readily apparent that comparing the keyed in security code, i.e. password, keystroke by keystroke with a predetermined primary security code, i.e. predetermined primary password, as required by the Lewis patent using the Sibigtroth, et al. patent's data processing system 10 requires that the peripheral portion 12 must provide the keyed in security code to the integrated circuit package portion 11.

38. Referring again to Exhibit A, it is also readily apparent that even when the integrated circuit package portion 11 operates either in its "secure mode" or in its "single chip" mode, an ICE connected to the integrated circuit package portion 11 can monitor and record, via the address bus 22 which extends from inside the integrated circuit package portion 11 outside to the peripheral portion 12, all addresses from which the data processor 14 fetches data and instructions from the memory 13.

39. Since col. 3, lines 50-53 of the Lewis patent discloses that the microcomputer 10 compares the keyed in security code, i.e. password, keystroke by keystroke with a predetermined primary security code, if a Sibigtroth-style microcomputer 10 stored the Lewis patent's predetermined primary security code, i.e. predetermined primary password, in its memory 13, and if the Sibigtroth-style microcomputer 10 were operating in its "secure mode,"[3] by monitoring the address bus 22 an ICE connected to the integrated circuit package portion 11 can record all addresses in the memory 13 from which the data processor 14 fetches data and instructions while comparing keystroke by keystroke the keyed in security code, i.e. password, with the predetermined primary security code, i.e. predetermined primary password stored in the memory 13.

40. Using an ICE, having thus monitored and recorded all addresses in the memory 13 from which the data processor 14 fetches data and instructions while comparing keystroke by keystroke the keyed in security code, i.e. password, with the predetermined primary security code, i.e. predetermined primary password, one could then readily ascertain the predetermined primary security code, i.e. predetermined primary password, by operating the integrated circuit package portion 11 in its "expanded mode" and exporting from the integrated circuit package portion 11 to the ICE

[3] Note that if the Sibigtroth-style microprocessor 10 were operating in its "single chip mode," it could not receive via the data/instruction bus 30 a "keyed in security code."

the data stored in the memory 13 at the address previously monitored and recorded using the ICE.

41. Thus, constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action merely makes ascertaining the predetermined primary security code, i.e. predetermined primary password, a two step operation, i.e. first record the addresses in the memory 13 and then obtain from the memory 13 the data stored at those addresses, rather than a one step operation.

42. Furthermore, constructing the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action and storing the predetermined primary security code, i.e. predetermined primary password, in the memory 13 of the integrated circuit package portion 11 fails to provide non-volatile password storage.

43. Consequently, if one were to construct the microcomputer 10 of the Lewis patent in the method of the Sibigtroth, et al. patent as suggested at the bottom of page 4 in the January 14, 2004, Office Action and were to store the predetermined primary security code, i.e. predetermined primary password, in the memory 13 of the integrated circuit package portion 11, due to a lack of non-volatile storage the predetermined primary security code, i.e. predetermined primary password, would be forever lost if electrical power were removed from the integrated circuit package portion 11.

44. I am unaware of any facts contrary to the facts and opinions contained in this Declaration.

45. I declare under penalty of perjury under the laws of the United States of America that all statements made herein of my own knowledge are true and correct, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of any patent issuing on the subject application.

Brian Oh

Brian Oh

Dated: 2-17, 2004

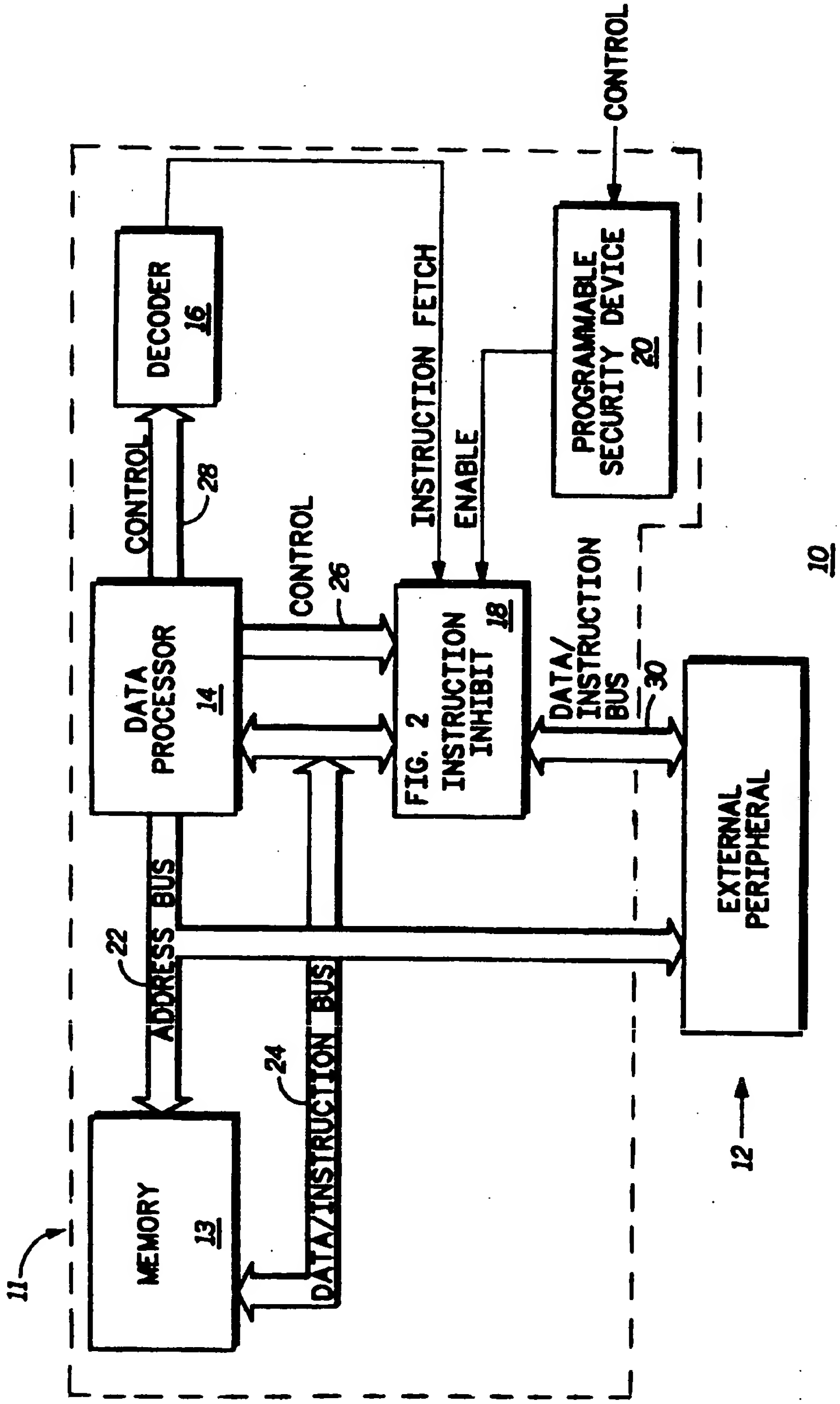
CONTROL
DECODER
16
PROGRAMMABLE SECURITY DEVICE
20
INSTRUCTION FETCH
ENABLE
CONTROL
28
CONTROL
26
DATA PROCESSOR
14
FIG. 2 INSTRUCTION INHIBIT
18
DATA/ INSTRUCTION BUS
30
10
EXTERNAL PERIPHERAL
22
ADDRESS BUS
24
DATA/INSTRUCTION BUS
MEMORY
13
11
12

FIG.1